PENTESTING “PRUEBA DE PENETRACIÓN” PARA LA IDENTIFICACIÓN DE VULNERABILIDADES EN LA RED DE COMPUTADORAS EN LA ALCALDÍA DEL MUNICIPIO DE CANTÓN DEL SAN PABLO, DEPARTAMENTO DEL CHOCÓ

AUTOR:

ING. JHON EDINSON VALDERRAMA GUARDIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

QUIBDÓ-CHOCÓ

2017

PENTESTING “PRUEBA DE PENETRACIÓN” PARA LA IDENTIFICACIÓN DE VULNERABILIDADES EN LA RED DE COMPUTADORAS EN LA ALCALDÍA DEL MUNICIPIO DE CANTÓN DEL SAN PABLO, DEPARTAMENTO DEL CHOCÓ

JHON EDINSON VALDERRAMA GUARDIA

PROYECTO PARA OBTENER EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ASESOR ENCARGADO

ING. FERNANDO JOSÉ DÍAZ MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA– UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

QUIBDÓ-CHOCÓ

2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

DEDICATORIA

A mis padres que lo han dado todo por mí y especialmente a mi madre que es mi Inspiración y mi compañía siempre.

A Yisel Renteria, mi mujer, mi compañera y amiga que siempre me ha apoyado en todos los proyectos que como familia hemos iniciado siempre afrontando cada situación de la mejor forma posible.

A mis hijos Santhiago y Eliam que le dan sentido a mi vida y que siempre está en mi corazón con su amor.

AGRADECIMIENTOS

Agradezco a mis padres por enseñarme a luchar por mis sueños, por enseñarme los que me ayudan a comportarme en sociedad, gracias por eso y todos los esfuerzos que realizaron para sacarme adelante.

A mis hermanos por apoyarme en cada decisión que tomo, y por estar a mi lado en cada momento hoy, mañana y siempre.

A mis hijos Daniel santhiago y Eliam andres Valderrama Rentería que me llenan de la fuerza suficiente para salir adelante.

A todas las personas que me incentivaron y me motivaron para seguir adelante con los objetivos de este propósito y luchar por una meta más.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

ANEXOS

Pág.

INTRODUCCIÓN

En la actualidad el uso de equipos tecnológicos ha integrado a toda la humanidad de una manera vertiginosa, hecho asociado a las redes de computadoras y la interconectividad de estas con el servicio de internet, lo que ha conllevado a un hecho fundamental que ha proporcionado relevancia a la seguridad informática, en este mundo especializado de información que viaja a través de los diferentes servicios de la red, como son, el enviar un correo electrónico, abrir un documento remoto, participar en una webconference, tener una sesión de chat, comunicación de voz sobre IP, todo esto requiere de estrategias y métodos de protección informática.

Enfatizando en la importancia de la información de las entidades y empresas, esta se convierte en el patrimonio intangible más valioso, la cual genera mucho interés en los intrusos informáticos para cometer hechos delictivos, proceso en el cual se deben de tomar todas las precauciones técnicas y tecnológicas en la identificación de las vulnerabilidades de la red computadores y sus servicios.

Los administradores de Sistemas de información, tiene muchas responsabilidades funcionales, pero la más importante es mantener la seguridad de la red lo menos vulnerable y amenazada posible, para esto es importante que constantemente pongamos a prueba los métodos de seguridad que tenemos implementado y además podamos detectar cualquier vulnerabilidad que exista antes de que esta sea aprovechado por un delictivo informático.

Un PenTesting “Prueba de Penetración”, “permite generar acciones de protección informática, la cual consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social. El objetivo de estas pruebas es verificar bajo situaciones extremas cuál es el comportamiento de los mecanismos de defensa específicamente, y se busca detectar vulnerabilidades en los mismos. Además, se identifican aquellas faltas de controles y las brechas que pueden existir entre la información crítica y los controles existentes”[1].

El Pentesting que se aplicara, se realizara en base a la red y a los servicios que corren en ella, incluyendo los servidores, permitiendo hacer pruebas de: Sistemas Criptográficos, Contraseñas, Sistemas Operativos, Servidores Web, Firewell, detectores de Intruso, Redes Inalámbricas y Sistemas de Bases de datos.

[1] Mauro Maulini (21 de Agosto de 2012). Penetración Test, ¿En qué consiste? Tomado de: https://hackersenlared.wordpress.com/category/capacitacion/que-es-un-pentest/

1. PROBLEMA DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La Alcaldía del Municipio de Cantón del san pablo, Departamento del Chocó, es una entidad del estado, del orden territorial y a favor de la comunidad, cuyo objetivo es velar y prestar sus servicios públicos con el cumplimiento de un rol fundamental para con la población, ya que como institución pública, autónoma y jurídicamente hablando, puede promover e implementar toda clase de actividades políticas, económicas, sociales y culturales, con la visión de satisfacer las necesidades de la comunidad.

El ente territorial en su principio de actualización e inmersión tecnológica para todos y cada uno de los procesos que se generan funcionalmente, ha implementado un sistema distribuido de red de computadoras LAN (Local Área Network) la cual permite compartir recursos Software, Hardware e información, elementos que deben contar con confidencialidad, Integralidad y disponibilidad.

Dicha situación conlleva a una nefasta perdida, robo o destrucción de la información, suplantación de identidad de funcionarios, virus informáticos, fallos en los sistemas de información, mal funcionamiento del Hardware, intermitencia o caída de la red (offnet), Spoffing de DNS, IP o DCHP, denegación del servicio (DoS), ingeniería social, entre otras situaciones críticas que afectan el funcionamiento de una red y sus servicios.

1.2. **JUSTIFICACIÓN DEL PROBLEMA**

El desarrollo de esta investigación le permitirá a la Alcaldía del Municipio de Cantón del san pablo, contar con red de computadoras y sus respectivos servicios de forma segura, permitiendo generar un alto grado de confidencialidad, Integralidad y disponibilidad de la información.

Los análisis de vulnerabilidades o PenTesting permitirán determinar el nivel de seguridad en: un equipo, en la red de equipos LAN (Local Área Network) o WLAN (Wireless local Área Network), aplicaciones Web, Servidores de Información, entre otros, por medio de ataques informáticos simulados idénticos a los que realizaría un Cracker o Black Hat Hacker pero sin poner en riesgo la información o la disponibilidad de los servicios, esto se hace con el fin de encontrar las posibles amenazas o vulnerabilidades en los sistemas informáticos antes de que las descubra un atacante (externo o interno). (Burker , 2012)

El Pentesting “Prueba de penetración” a la red de computadoras y sus servicios de la Alcaldía del Municipio de Cantón del san pablo, en el Departamento del Chocó, permitirá explorar la red, realizar análisis de seguridad, auditoría de red y búsquedas de puertos abiertos en la máquina remota. Además, permite entre otros aspectos analizar la red en busca de hosts (PC) en directo, sistemas operativos, filtros de paquetes y puertos abiertos que se ejecutan en máquinas remotas convirtiéndose en eventuales vulnerabilidades. El procedimiento para la identificación de las vulnerabilidades en la red de computadores y

sus servicios en la Alcaldía del Municipio de Cantón del San Pablo, incluye específicamente cuatro etapas o procedimientos.

La primera etapa o descubrimiento, es donde se delimitara las áreas donde se focalizara la evaluación, que para este caso es la red de computadoras y sus servicios en la alcaldía de Cantón de san pablo, Departamento del Chocó y para ello es necesario realizar la recolección de información necesaria, tales como: rangos de direcciones IP asignados, direcciones IP de servicios, dirección física de la alcaldía, nombres de funcionarios y cuentas de correo electrónico, fuentes de información, análisis de la página WEB y existencia de redes inalámbricas (WiFi).

Para la segunda etapa o exploración, se trazan los objetivos para las demás etapas y se aplican técnicas no invasivas para identificar todos los blancos potenciales existentes en la red. Además se deberá incluir el análisis de protocolos, relevamiento de plataforma y barreras de protección, scanning de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web.

Para esta etapa, las tareas que predominan son: Detección de módems activos, Confirmación de rangos de direcciones IP, detección de equipos activos e identificación de Sistemas Operativos, detección de servicios activos e identificación Software y versiones, detección de barreras de protección y análisis de características de configuración en redes WiFi.

En la tercera etapa o evaluación, se realizan los análisis de todos los datos encontrados para la identificación de las diferentes vulnerabilidades. Durante esta fase se desarrollan los diferentes informes de las pruebas realizadas y se detallan las vulnerabilidades encontradas.
Análisis de resultados obtenidos de la red de computadores e identificación de las vulnerabilidades.
Esta fase se desarrollará mediante la construcción de un informe que presente un análisis de los resultados de la prueba y detalle las vulnerabilidades encontradas en el mismo

Para culminar, en la cuarta etapa o Intromisión, se buscan alternativas que permitan acceder a los sistemas y obtener el control de los mismos.
Entre las pruebas que se ejecutan para la evaluación de las vulnerabilidades en la red de computadores y sus servicios en la Alcaldía del Municipio de Cantón de san pablo, se tiene: pruebas a sistemas criptográficos, pruebas a contraseñas, pruebas a los sistemas operativos, pruebas a servidores (WEB, FTP, SMTP, ICMP), pruebas a los Firewalls, pruebas a los IDS (Detectores de intrusos), pruebas a los sistemas de base de datos (Mysql, JavaDB, SqlServer) y pruebas a las redes inalámbricas. (Ramos Ramos)

Con la identificación de los elementos o epatas anteriores, y la aplicación de las respectivas pruebas, se establecería la reducción de las vulnerabilidades, además del establecimiento de estrategias de prevención de ataques informáticos, generando capacitación, orientación y actualización de los funcionarios en temas de seguridad informática.

Finalmente, el desarrollo de las pruebas de penetración permitió conocer las vulnerabilidades a las que se encuentra sometida la red permitiendo así realizar trabajos correctivos que generen un mejor funcionamiento en el ámbito de la seguridad informática.

1.3. FORMULACIÓN DEL PROBLEMA

¿Cómo identificar el nivel de seguridad de la red de computadoras en la Alcaldía del Municipio de Cantón de san pablo, Departamento del Chocó mediante la ejecución de pruebas de penetración y generar más seguridad en la Alcaldía y equipos de cómputos?

1.4. OBJETIVOS

1.4.1. General

Describir los problemas de seguridad de la red de computadoras en la alcaldía del municipio de Cantón de san Pablo, a través de pruebas de penetración que permitan el mejoramiento continuo de la entidad.

1.4.2. Específicos

- Realizar un pentesting “prueba de penetración” para la determinar qué tipo de vulnerabilidades presenta la red de computadoras en la alcaldía del municipio de Cantón de san Pablo, departamento del Chocó.

- Identificar los diferentes ataques a los que está expuesta la red de computadoras y sus servicios.
- Generar recomendaciones que reduzcan la vulnerabilidad de la red de computadoras.

2. MARCO DE REFERENCIA

2.1. MARCO CONTEXTUAL.

El municipio del Canton del Pablo se encuentra ubicado en la parte noroccidental del Departamento del Choco en la República de Colombia, tiene una extensión de 386 km2 y una densidad demográfica de 16.39 habitantes /km2, su cabecera Municipal es Managru, está localizada a los 50° 20 20" de latitud norte y 76º 43’53" de longitud oeste, su altura sobre el nivel del mar es de 57 m, la temperatura media 270C. Dista de Quibdó 60 Km. El Cantón limita: por el Norte con Quibdó, Río Quito y Alto Baudó, por el Este con Cértegui, Unión Panamericana, por el Sur con Istmina y por el Oeste con Alto Baudó y Medio Baudó; su jurisdicción político administrativa esta integrada por ocho corregimientos así: Managrú; Puerto Pérvel; Taridó; La Victoria; Guapandó; Boca de Raspadura, la Isla y Pavaza; cuatro veredas, Duana, Puerto Juan, Tuadó y San José de Quite El territorio es ondulado hacia la parte occidental, sus alturas no sobrepasan los 150 m sobre el nivel del mar; la región oriental es ondulado y corresponde a la serranía del Baudó; lo bañan los, ríos San Pablo, Cértegui y Taridó. Sus tierras se distribuyen en el piso térmico cálido, tiene una temperatura media de 28°C. Administrativamente, pertenece al círculo notarial, a la oficina seccional de registro de Istmina, y al circuito judicial de Tadó, corresponde a la circunscripción electoral del Chocó.

Según el CENSO 2005 la población del cantón es de 4.413 habitantes, el consolidado a junio 30 de 2005, presenta una población del municipio Cantón del San Pablo con 6.213

habitantes; para el 2007 la población proyectada fue de 6.335 discriminada así: el 49% conformada por mujeres y el 51% por hombres.[2]

2.2. MARCO TEÓRICO

2.2.1. Seguridad Informática

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. [3]

La seguridad informática se encarga del diseño de normas que están dirigidas a establecer condiciones de seguridad para el tratamiento de datos en un sistema informático.

Actualmente se considera que la seguridad de los datos y la información comprenden 3 aspectos fundamentales:

- Confidencialidad
- Integridad (seguridad de la información)
- Disponibilidad

[2] Delimitaciones (2017). Tomado de: http://www.elcantondesanpablo-choco.gov.co
[3] Seguridad Informática SMR (2014). Tomado de: http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

Disponibilidad*:* Hace referencia a la capacidad de un sistema que permite realizar consultas en la medida que se requiera de una manera rápida y eficaz por el personal autorizado. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

Confidencialidad: hace referencia a la privacidad de la información, la seguridad informática debe proteger un sistema informático de acceso a la información por parte de personal o programas no autorizados.

Integridad*:* Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Hace referencia a la veracidad y validez de los datos almacenados o guardados en un sistema informático.

Las amenazas.

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que permite al atacante tener total control de nuestra máquina robando así nuestros datos y demás.

Amenazas lógicas:

Software incorrecto: (a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.)

Herramientas de seguridad*:* (permiten a los administradores detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras*:* Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial[4].

Canales cubiertos: son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.

Virus*:*(un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas permitiendo el control y la denegación del servicio para el usuario de esa máquina.)

Gusanos:(es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su número no es muy elevado pero el daño que causa es muy grave.)

[4] Seguridad Informática SMR (2014). Tomado de: http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

Caballos de Troya*:* (son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera del pero que realmente ejecuta funciones ocultas).

Amenazas Físicas:

Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales.

Formas de protección de nuestro sistema: Para proteger nuestros sistemas hemos de realizar un análisis de las amenazas potenciales, las pérdidas que podrían generar y la probabilidad de si ocurrencia a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan, a esto se le llama mecanismo de seguridad, son la herramienta básica para garantizar la protección de los sistemas o la red. Estos mecanismos se pueden clasificar en activas o pasivas.

Activas*:* evitan daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software específico en seguridad informática.

Pasiva*:* minimizan el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.[5]

2.2.2. **Redes de computadoras**

Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.[6]

Algunos expertos creen que una verdadera red de computadoras comienza cuando son tres o más los dispositivos y/o computadoras conectadas.

Para comunicarse entre sí en una red el sistema de red utiliza protocolos de red.

Por extensión las redes pueden ser:

- Área de red local (LAN)
- Área de red metropolitana (MAN)
- Área de red amplia (WAN)
- Área de red personal (PAN)

[5] Manual de buenas prácticas y recomendaciones (2017). Tomado de: http://www.informaticarubinos.com/windows/wp-content/uploads/2017/01/manual-buenas-praticas.pdf

[6] Alegsa, Diccionario de red de Informática y tecnología (2014). Tomado de: http://www.alegsa.com.ar/Dic/red%20de%20computadoras.php

Por relación funcional se clasifican en:

- Cliente/Servidor
- igual-a-igual (P2P)

Por topología:

- Red alambrada
- Red de anillo
- Red de bus
- Red de bus-estrella
- Red de estrella
- Red Mesh

Por estructura:

- Red OSI
- Red TCP/IP

2.2.3. **Equipos de una Red de Computadores**

Entre los equipos que se interconecta en una red de computadores, tenemos los siguientes:

Router

En español, enrutador o encaminador. Dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red).

Switch

Un switch es un dispositivo electrónico de interconexión de redes de ordenadores.
El objetivo principal es interconectar dos o más segmentos de red, funcionando de manera similar a los puentes (bridges).

Modem

Un modem es un dispositivo que permite convertir las señales digitales en señales analógicas o viceversa, esta conversión es necesaria para poder trasmitir la seña a través de canales de comunicación como las líneas telefónicas, cables coaxiales, fibras ópticas y microondas.

Servidor

Un servidor es un tipo de software que permite realizar algunas tareas requeridas por los usuarios. Cuando se habla de servidores también podemos referirnos a un ordenador físico en el cual funciona el software que tiene como propósito proveer datos de modo que otros usuarios puedan utilizarlos.

Firewall

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red

Hub

En informática un hub o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás[7].

2.3. **ANTECEDENTES**

Realizar Pentesting "pruebas de penetración" es una tarea compleja, involucra un proceso en donde se realizan distintos tipos de tareas que identifican, en una infraestructura objetivo, las vulnerabilidades que podrían explotarse y los daños que podría causar un atacante. En otras palabras, se realiza un proceso de hacking ético para identificar qué

[7] Introducción a las redes (2010). Tomado de: https://claudiooq2.wordpress.com/switch-hub-router-bridge/

incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de tal forma que se eviten estos ataques.[8]

A continuación se relacionan otras investigaciones relacionadas:

2.3.1. **Metodología para la Detección de Vulnerabilidades en Redes de Datos**

Título: Methodology for Detecting Vulnerabilities in Data Networks

Autor: Franco, David A ; Perea, Jorge L ; Puello, Plinio

Temas: Detección De Vulnerabilidades ; Enumeración de Servicios ; Escaneo de Puertos ; Seguridad Informática ; Vulnerability Detection ; Service Enumeration ; Port Scanning ; Information Security

En: Información tecnológica, 2012, Vol.23 (3), pp.113-120 [Revistas arbitradas]

Descripción: este trabajo tuvo como objetivo principal diseñar una metodología que permita la detección de vulnerabilidades e n las redes de datos.

2.3.2. **Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios**

Título: Vulnerability Detection Tool using Banner Grabbing

[8] Seguridad de la Información (2017). Tomado de: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Autor: Franco, David A ; Perea, Jorge L ; Tovar, Luis C

Temas: Vulnerabilidad De Redes ; Servicios De Red ; Seguridad ; Pruebas De Penetración ; Identificación De Servicios ; Network Vulnerabilities ; Network Services ; Security ; Penetration Test ; Banner Grabbing

En: Información tecnológica, 2013, Vol. 24(5), pp.13-22 [Revistas arbitradas]

Descripción: El objetivo principal de este trabajo fue diseñar un nuevo enfoque para la detección y evaluación de vulnerabilidades en equipos de red mediante la técnica de identificación de servicios. Este enfoque consiste en determinar los nombres y versiones de los servicios activos en un equipo de red para luego buscar las vulnerabilidades de seguridad de los mismos en la Base de Datos Nacional de Vulnerabilidades.[9]

2.3.3. **Fundamentos prácticos de seguridad en redes inalámbricas IEEE 802.11**

"Título: Fundamentos prácticos de seguridad en redes inalámbricas IEEE 802.11 Basic security measures for IEEE 802.11 wireless networks

Autor: Sarmiento Oscar P. ; Guerrero Fabio G. ; Rey Argote David

Temas: 802.11i ; 802.1x ; Ccmp ; Tkip ; Wep ; Wlan ; Wpa ; Wpa2.

En: Ingeniería e Investigación, 2008, Vol.28(2), p.89

Descripción: Este artículo presenta una discusión tutorial de tres estándares de seguridad de uso común en las redes inalámbri-cas IEEE 802.11: WEP, WPA y WPA2. Se realiza un análisis detallado del algoritmo RC4 que soporta a WEP y se in-dican sus vulnerabilidades.

[9] INFORMACION TECNOLOGICA VOL. 24 No. 5 (2013) https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642013000500003.

También se revisan los aspectos y características técnicas más relevantes de los protocolo de cifrado WPA y WPA2 con la finalidad de hacer un análisis comparativo de los tres estándares en términos de la seguridad que ellos proporcionan. Se ha dado especial atención al aspecto didáctico del funcionamiento del ci-frado WEP mediante el desarrollo y uso de una herramienta de simulación escrita en C++ Builder para facilitar su comprensión a nivel académico. Igualmente, se presentan dos casos prácticos de seguridad de red inalámbrica con equipos del fabricante Cisco, habilitando y configurando WPA Personal y WPA2 Personal, opciones de seguridad que usan TKIP y AES, respectivamente. "[10]

2.4. **MARCO LEGAL**

2.4.1. **Normatividad Internacional**

2.4.2. **Estándar ISO/IEC 17799**

"Debido a la necesidad de hacer segura la información que poseen las organizaciones era necesaria la existencia de alguna normativa o estándar que acogiera todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudieran afectarla por esta necesidad apareció el BS 7799, o estándar para la gestión de la seguridad de la información, el cual es un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la

[10] REVISTA INGENIERÍA E INVESTIGACIÓN VOL. 28 No. 4 (2, AGOSTO DE 2008) https://www.researchgate.net/publication/238068275_Fundamentos_practicos_de_seguridad_en_redes_inalambricas_IEEE_8021

organización. Esta normativa británica acabó desembocando en la actual ISO/IEC 17799:2000 – Code of Practice Information Security Management."[11]

ISO/IEC 17799 (también ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Orgnization For Standardization y por la Comisión International Electrotechnical Commission en el año 2000 y con el título de Information Technology - Security Techniques - Code of Practice For Information Security management. La actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

2.4.3. **Estándar ISO/IEC 27001**

"Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI)."[12]

[11] JOLMAN, ALEXANDER. (25 de Febrero de 2012) Seguridad Informática. Tomado de: http://jrobledoherrera.blogspot.com/2009/02/seguridad-informatica.html.

[12] ISO (INTERNATIONAL ORGANIZATION OF ESTANDARDIZATION). ISO/IEC 27001:2005. (28 de Febrero de 2012) Tomado de: http://www.iso.org/iso/catalogue_detail?csnumber=42103.

"La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de disponer de la certificación según ISO/IEC 27001 ayuda a gestionar y proteger los valiosos activos de información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI."[13]

2.4.4. **Estándar ISO/IEC 27000:2009**

Es parte de una familia en crecimiento de Estándares para Sistemas de Administración de Seguridad de la información (ISMS), las "series ISO/IEC 27000".

ISO/IEC 27000, es un estándar internacional titulado "Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario"

[13] BSI (British Standards Institution 2012). Seguridad de la Información ISO/IEC 27001. Tomado de: http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/.

El estándar fue desarrollado por el sub-comité 27 (SC27) del primer Comité Técnico Conjunto (JTC1), de la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission)

ISO/IEC 27000 provee:

- Una vista general a la introducción de los estándares de la familia ISO/IEC 27000
- Un glosario o vocabulario de términos fundamentales usados a lo largo de toda la familia ISO/IEC 27000

La Seguridad de la Información, como muchos otros temas técnicos, está desarrollando una compleja red de terminología. Relativamente pocos autores se toman el trabajo de definir con precisión lo que ellos quieren decir, un enfoque que es inaceptable en el campo de los estándares, porque puede potencialmente llevar a la confusión y a la devaluación de la evaluación formal y la certificación[14].

El alcance de ISO/IEC 27000 es "especificar los principios fundamentales, conceptos y vocabulario para la serie de documentos ISO/IEC 27000"

ISO/IEC 27000 contiene, en otras palabras:

Una vista general de los estándares ISO/IEC 27000, mostrando cómo son usados colectivamente para planear, implementar, certificar, y operar un Sistema de Administración de Seguridad de la información, con una introducción básica a la Seguridad de la Información, administración de riesgos, y sistemas de gestión.

[14] Seguridad Informática (2014). Tomado de: https://seguridadinformaticaufps.wikispaces.com/Normatividad+en+la+Seguridad+Inform%C3%A1tica

Definiciones cuidadosamente redactadas para temas relacionados con seguridad de la información.

ISO/IEC 27000 es similar a otros vocabularios y definiciones y con suerte se convertirá en una referencia generalmente aceptada para términos relacionados con seguridad de la información entre ésta profesión.

2.5. NORMATIVIDAD NACIONAL

2.5.1. Ley 1273 del 2009 Delitos Informáticos

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley decreta:[15]

2.5.2. Capítulo I:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

- *Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático.

[15] Secretaria general de la Alcaldía Mayor de Bogotá (5 de Enero de 2009). Ley 1273 de 2009. Tomado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- *Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.
- *Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.
- *Artículo 269D: DAÑO INFORMÁTICO.* El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.
- *Artículo 269E: USO DE SOFTWARE MALICIOSO.* El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
- *Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.* El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes
- *Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.* El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fé.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

2.5.3. **Capitulo II:**

De los atentados informáticos y otras infracciones:

- *Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.* El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

- *Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

2.6. MARCO CONCEPTUAL.

Arp. Protocolo de resolución de direcciones a nivel de capa de red responsable de encontrar la dirección MAC que corresponde a una dirección IP.

Atacante. Persona con conocimientos informáticos que está acechando un sistema.

Ataque. Es un proceso dirigido por un atacante a través de un programa intenta ingresar a un sistema.

Auditoría. Es un estudio que se encarga de analizar e identificar vulnerabilidades.

Autenticación. Es el proceso de establecimiento y verificación de la identidad para realizar una petición.

Backtrack. Distribución de Linux para realizar un ethical hacking, contiene varias herramientas de hacking.

CERT. (Computer emergency response team) Equipo responsable para manejar los problemas concernientes a la seguridad informática.

Contraseña. Es una clave para la autenticación que tiene información secreta para el acceso.

Cracker. Persona con conocimiento de herramientas de hacking pero con fines maliciosos.

Criptografía. Proceso de transformar un test plano a un texto descifrado.

Denegación de Servicio. Es interrumpir el funcionamiento correcto de un servicio. Diccionario. Se trata de un conjunto de palabras contenidas un archivo.

Exploits. Este consiste en aprovechar errores de programación en una aplicación con el objetivo de tomar el control de un sistema o realizar una escalada de privilegios.

Firewall. Es un cortafuegos/ software para controlar las comunicaciones denegando o permitiendo.

FTP. (File Transfer Protocol) Protocolo de transferencia de archivos.

Fuerza Bruta. Ataque que utiliza diccionarios para realizar las comparaciones con la clave a buscar.

Hacker. Individuo con conocimientos informáticos pero no tiene intenciones maliciosos y es apasionado a la seguridad informática

HTTP. (HiperText transfer protocol) protocolo perteneciente a la capa de aplicación usada par a las transacciones world wide web.

HTTPS. (HiperText transfer protocol Secure) es un protocolo basado en http, asegurando la transferencia de los datos.

IDS. Sistema de detección de intrusos que detecta accesos no autorizados a una red o computador.

Ingeniería Social. Técnica que se aprovecha la ingenuidad de las personas con el objetivo de obtener información.

IPS. Sistema de prevención de intrusos que previene accesos no autorizados. IPSEC. Protocolo Seguro sobre el protocolo IP.

Nessus. Herramienta para el análisis de vulnerabilidades.

Netbios. Protocolo que permite el establecimiento y mantenimiento de sesiones de comunicaciones entre computadores.

Nmap. Herramienta para el escaneo de puertos.

Ping. Comando que prueba el estado de conexión con un equipo.

Protocolo. Conjunto de reglas que establecen la comunicación entre dos computadoras.

SMB. Protocolo de red que permite compartir impresoras y archivos en red. Smb4k. Programa que permite examinar y montar recursos compartidos de la red. Smtp. Protocolo simple de transferencia de correo pertenece a la capa de aplicación se lo utiliza para el intercambio de mensajes de correo electrónico. Sniffers. Programa de captura de las tramas de red.

TCP. Protocolo de control de transmisión orientado a la conexión, ofreciendo mecanismos de seguridad en el proceso de comunicación.

TCP/IP. Modelo de descripción de protocolos de red Telnet. Protocolo que permite la conexión desde un terminal remoto.

Test de Penetración. Es un conjunto de metodologías y técnicas que permitan analizar debilidades de los sistemas informáticos.

Vulnerabilidad. Es una debilidad presente en cualquier sistema pudiendo ser explotada.

Xploit. Es un mecanismo que consiste en que la víctima recibe una postal falsa en su correo electrónico que contiene el link de una web falsa.

3. DISEÑO METODOLÓGICO

3.1. MARCO METODOLÓGICO

El proyecto de investigación se desarrollará tomando como punto de partida los elementos o fases de la investigación cualitativa. Determinando un alcance de procedimientos exploratorios, y teniendo en cuenta los diferentes métodos y técnicas propias de cada una de las etapas que se abordaran en el estudio, incluyendo los procedimientos, recolección, procesamiento y análisis de la información, además del seguimiento al cronograma de actividades.

La investigación se llevará a cabo en las siguientes fases o etapas que se describen a continuación:

3.1.1. **Fase I:**

Identificación de las diferentes fuentes de información que permitirán ampliar la perspectiva del conocimiento a aplicar. Se comenzará con la formulación de un instrumento tipo encuesta que contenga preguntas para los administradores del sistema tecnológico objeto de estudio, relacionadas con las características del mismo para así determinar la prueba de penetración que se debe realizar para la identificación de vulnerabilidades de la red de computadoras y sus servicios en la alcaldía de Cantón del San Pablo.

3.1.2. **Fase II:**

Selección y aplicación de las herramientas de Pentesting “Prueba de Penetración” para determinar técnicamente las vulnerabilidades de la red de computadoras.

Este procedimiento se realizará utilizando los programas Armitage y Nmap

3.1.3. **Fase III:**

Análisis de resultados obtenidos de la red de computadores e identificación de las vulnerabilidades.

Esta fase se desarrollará mediante la construcción de un informe que presente un análisis de los resultados de la prueba y detalle las vulnerabilidades encontradas en el mismo

3.1.4. **Fase IV:**

Aplicación de medidas correctivas y sugerencias para mitigar las vulnerabilidades de la red de computadoras.

Esta fase se desarrollará mediante la construcción de un protocolo que oriente a los administradores de la red de computadoras en cuestión sobre la forma de solucionar problemas como secuestro de información, afección por virus y otros. Así mismo, se entregan las recomendaciones de seguridad pertinentes para promover la seguridad permanente de la red.

3.1.5. **Fase V:**

Conclusiones y elaboración de un Documento final.

En este documento se recoge la sistematización completa del proceso de investigación, los logros y alcances, conclusiones y recomendaciones.

En la capacidad de ser asertivos en la investigación se emplearán técnicas de recolección de la información cuantitativas y cualitativas, tales como: La observación y la encuesta, al grupo de administradores de la red de computadores y los funcionarios entidad municipal con la finalidad de obtener los resultados más exactos con respecto a los problemas que se generan a través de las vulnerabilidades del sistema.

Para complementar la información requerida y recolectada es necesario tomar otras fuentes de información secundarias como la investigación a internet, material multimedia, libros o textos que tengan relación con el tema y el problema planteado, Inclusive todo material que direccione como fuente de solución al cumplimiento del objetivo.

4. DESARROLLO DEL PROYECTO

4.1. IDENTIFICACIÓN DE VULNERABILIDADES UTILIZANDO LA HERRAMIENTA ARMITAGE EN LA ALCALDÍA DEL CANTÓN DE SAN PABLO

Armitage es una herramienta instalada en Kali Linux, una distribución GNU/Linux en formato LiveCD esta distribución está diseñada para la realización de auditoria de seguridad. Es una distribución muy utilizada para el desarrollo de seguridad informática.

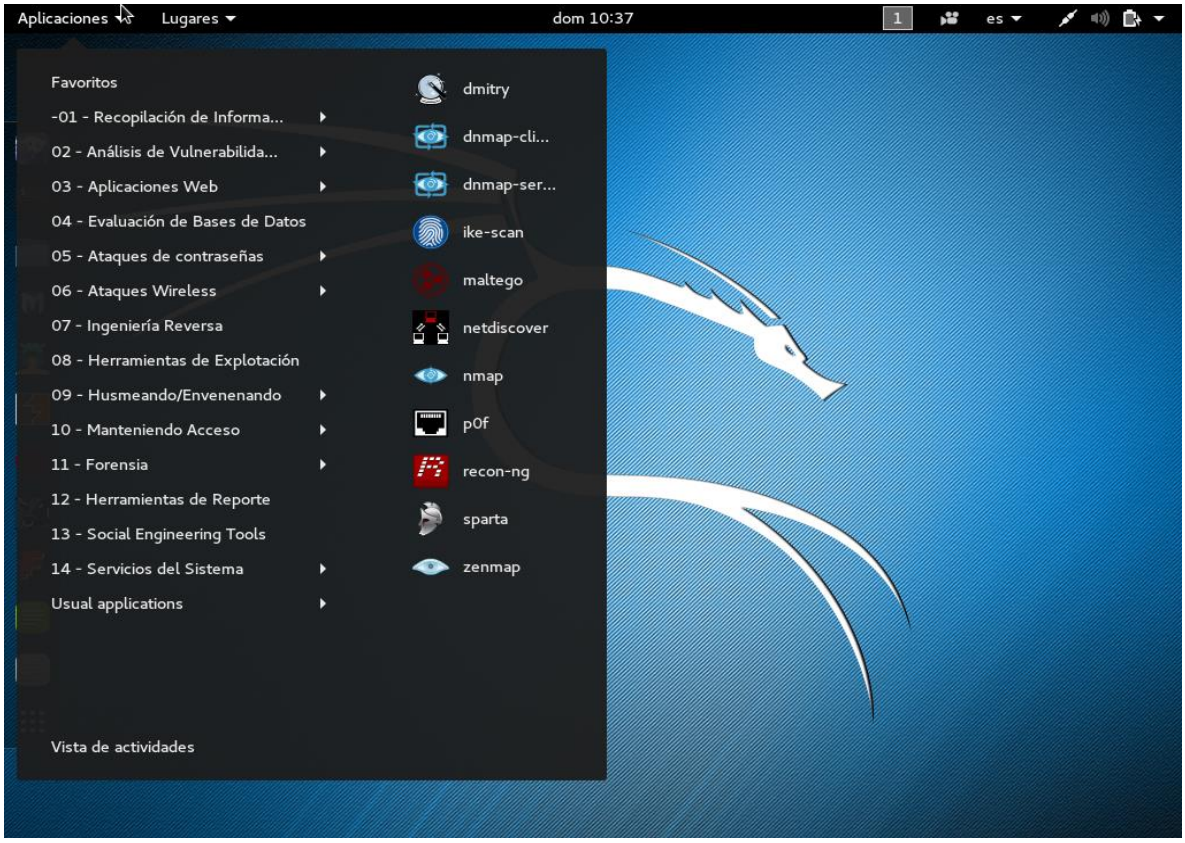
Dentro de las características que tiene esta distribución está el escaneo de puertos y vulnerabilidades en redes de datos, así como también escaneo de vulnerabilidades de bases de datos, herramientas para auditoria, herramientas de análisis forense, etc.

Para el desarrollo de esta investigación se utiliza la herramienta NMAP la cual se encuentra instalada en Kali Linux NMAP se usa para evaluar la seguridad de sistemas informáticos, así como también es utilizada para descubrir servicios en una red informática.

Es una de las herramientas más utilizadas por administradores de sistemas para pruebas de penetración también para verificar si hay servicios no autorizado ejecutándose, otros como los hacker o crackers lo utilizan para descubrir posibles objetivos de ataque.

NMAP, es una herramienta muy difícil de detectar por los sistemas de detección de intrusos es utilizado para realizar inventario de computadores en una red.

Figura 1 Kali Linux



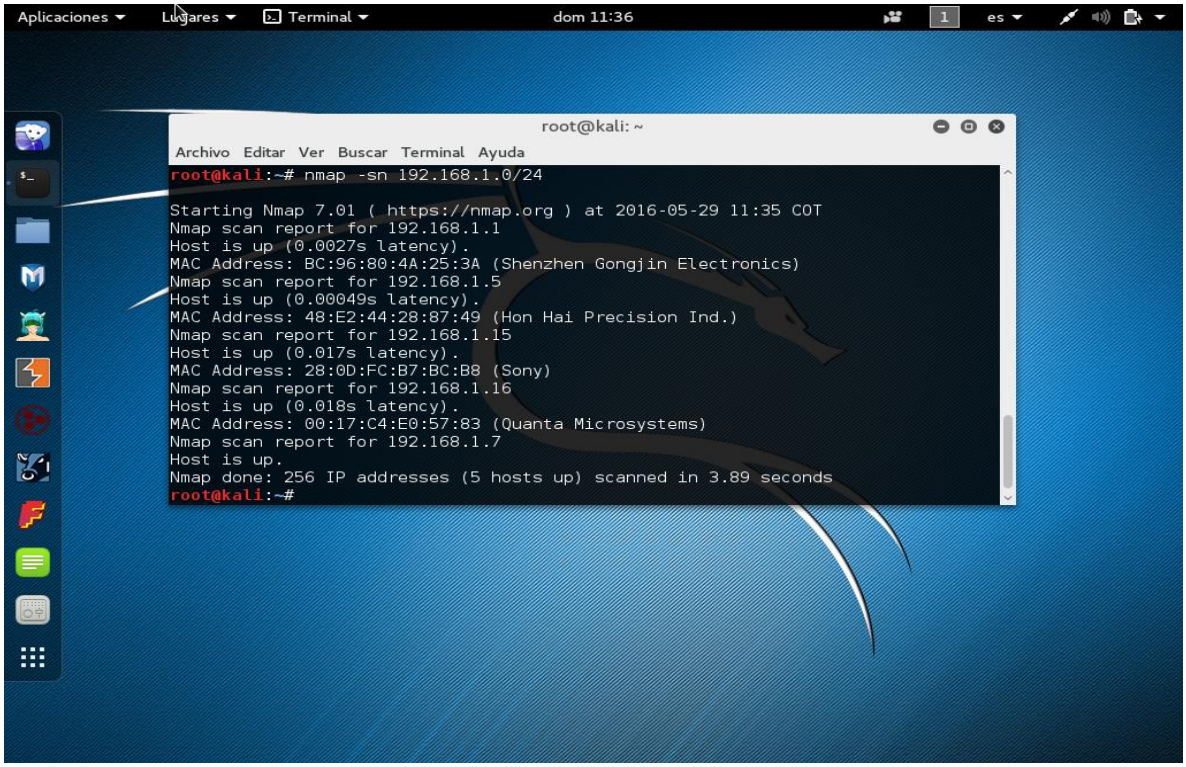
Tomada de: Autor

4.2. RECOLECTANDO INFORMACIÓN

El procedimiento se realiza desde la perspectiva de un hacker de sombrero blanco esto implica que la empresa auditada tiene conocimiento de los procesos a realizar examinar el rendimiento de la red y determinando que tan vulnerables son a ataques de intrusos la

información necesaria es suministrada por el administrador de la red de la alcaldía del Cantón de san pablo.

Figura 2 NMAP



Tomada de: Autor

La red de computadores de la alcaldía de Cantón de san pablo cuenta con un total de 17 equipos.

Por seguridad en el análisis de las vulnerabilidades algunos equipos de uso muy importante en las tareas de la alcaldía fueron dejados por fuera de esta prueba de seguridad.

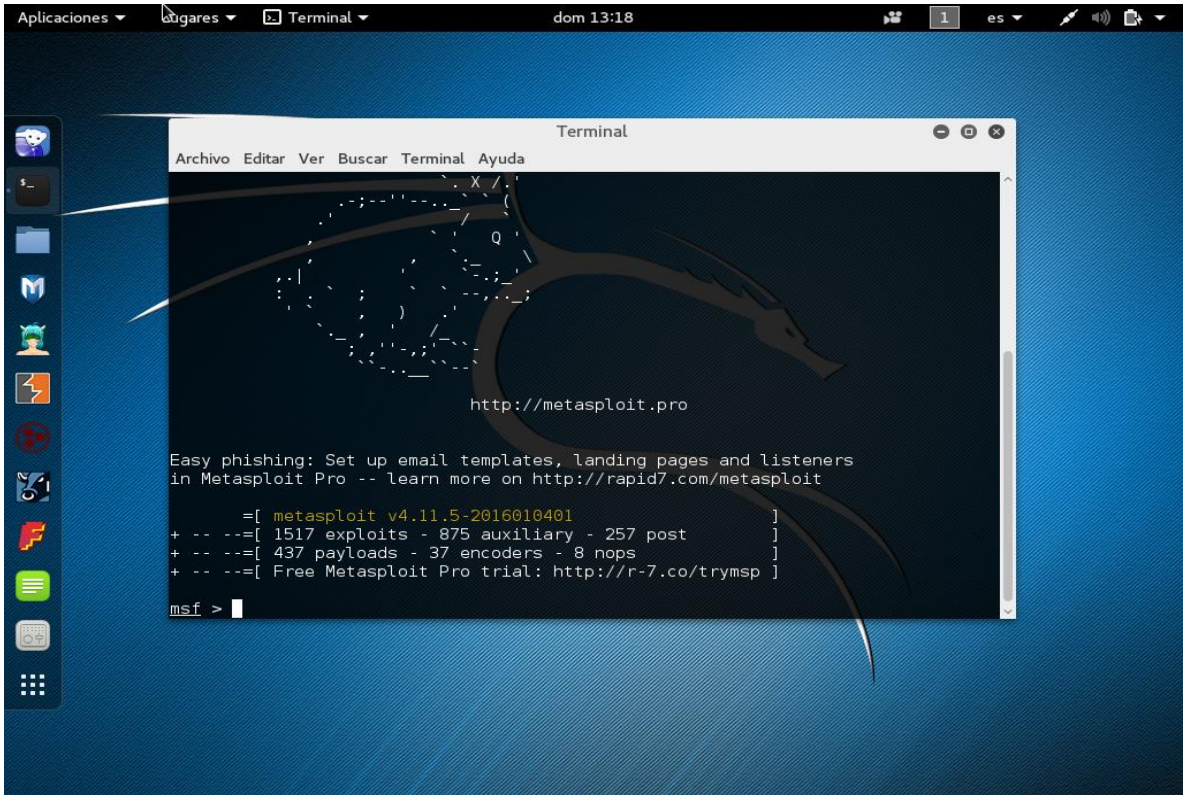
Después de identificar los diferentes dispositivos que hay en la red de la Alcaldía de Cantón de san pablo iniciaremos nuestra recolccion de informacion.

Una vez iniciada la sección en Kali Linux como administrador o root procederemos a abrir metasploit el cual nos permitirá utilizar diferentes archivos de penetración mediante la herramienta Armitage.

Metasploit: es una suite o conjunto de programas en realidad. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.[16]

[16] (Curso de Hacker, 2014)

Figura 3 Metasploit

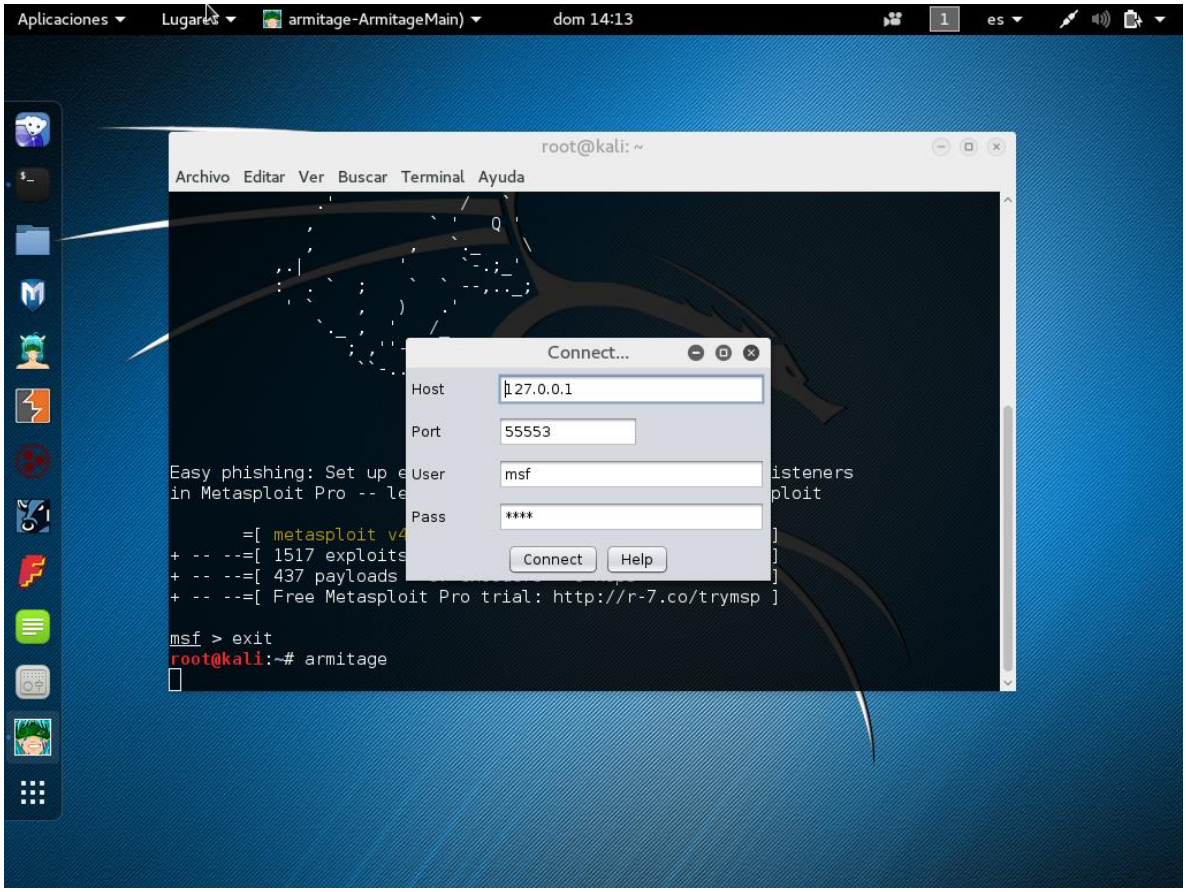


Tomada de: Autor

Para iniciar armitage debemos abrir una terminal y luego escribiremos armitage.

Iniciamos armitage dando click en conectar sin necesidad de tocar nada como se muestra en la figura 4.

Figura 4 Inciciando Herramienta Armitage



Tomada de: Autor

4.3. EXPLORACIÓN DE LA RED

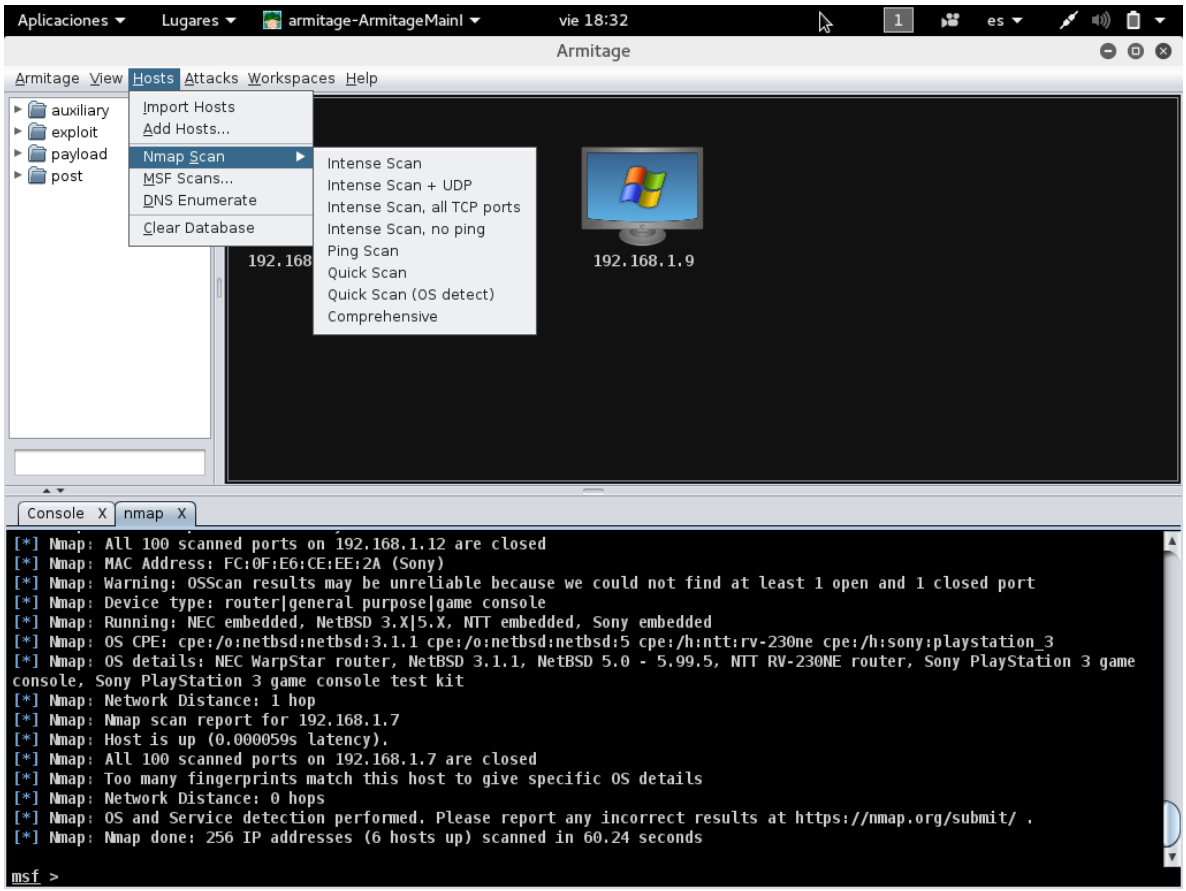
Para detectar los diferentes equipos con sus direcciones IP vamos a realizar los siguientes pasos como se puede evidenciar en la figura 5

1. Le daremos click en Hosts
2. Escogemos la opción Nmap Scan
3. Le damos click en Quick Scan (OS detect)

4. Esperamos que carguen los servicios de red.

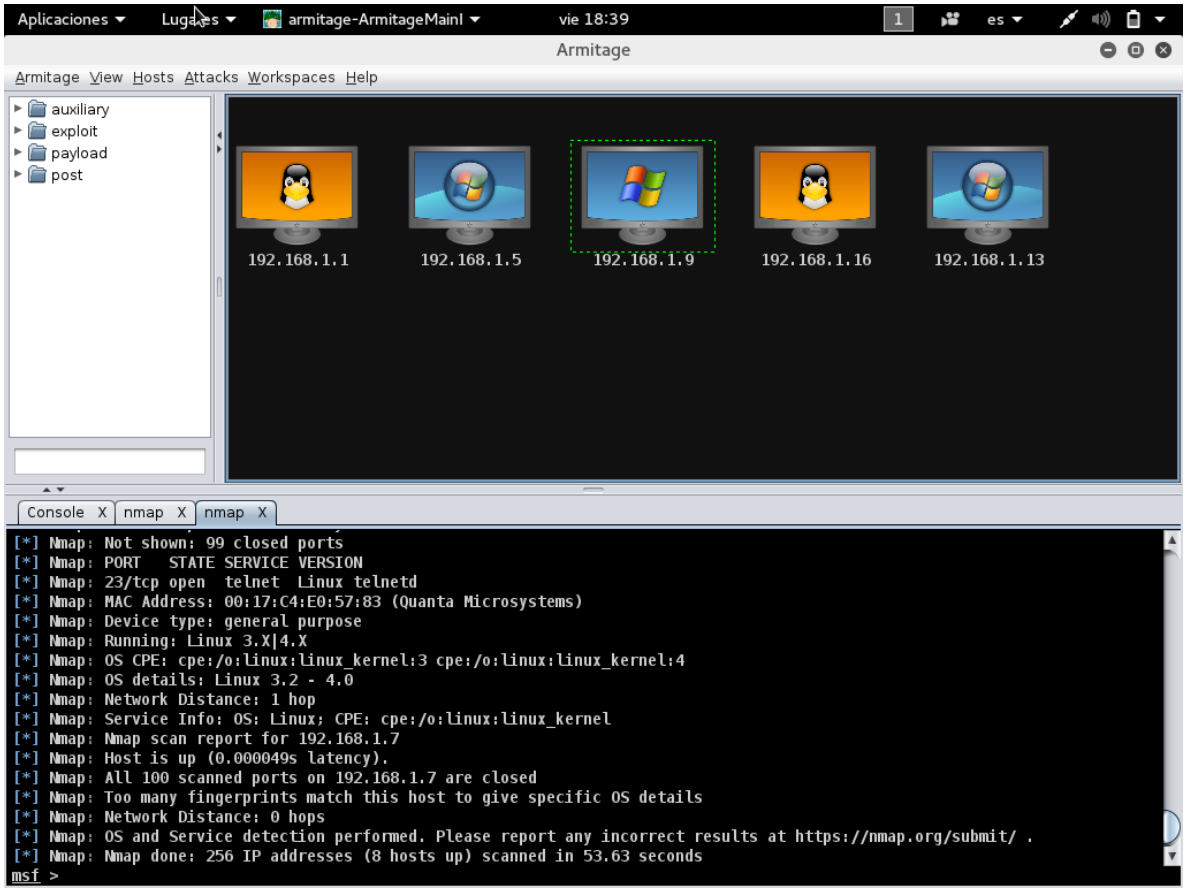
Este procedimiento nos permitirá la identificación de las diferentes IP los puertos y servicios disponibles en la red los diferentes sistemas operativos en la red de computadores de esta manera se visualizan los diferentes blancos a atacar para comprometer la red como se muestra en la figura 6.

Figura 5 Iniciando Escaneo



Tomada de: Autor

Figura 6 Equipos en Red



Tomada de: Autor

4.4. EVALUACIÓN DE LA RED

La exploración a la red red de computadores de la Alcaldía del Municipio de Cantón de San Pablo nos permite conocer los sistemas operativos que hay en ella de esta manera se hace más claro qué tipo de ataque realizar además nos permite conocer que maquina atacar debido a que tenemos conocimiento de la dirección IP de cada equipo en la red.

4.5. **ATACANDO LA RED**

Una vez realizado el escaneo de red este nos presentara los equipos en red intentaremos vulnerar primero el equipo de la secretaria de despacho el cual tiene por dirección IP la 192.168.1.9 y el sistema operativo que utiliza es Windows XP.

Para alistar el ataque vamos a seguir los siguientes pasos:

1. Seleccionaremos el equipo a atacar
2. Le damos click en la opción Attacks
3. Escogemos la opción Find Attacks

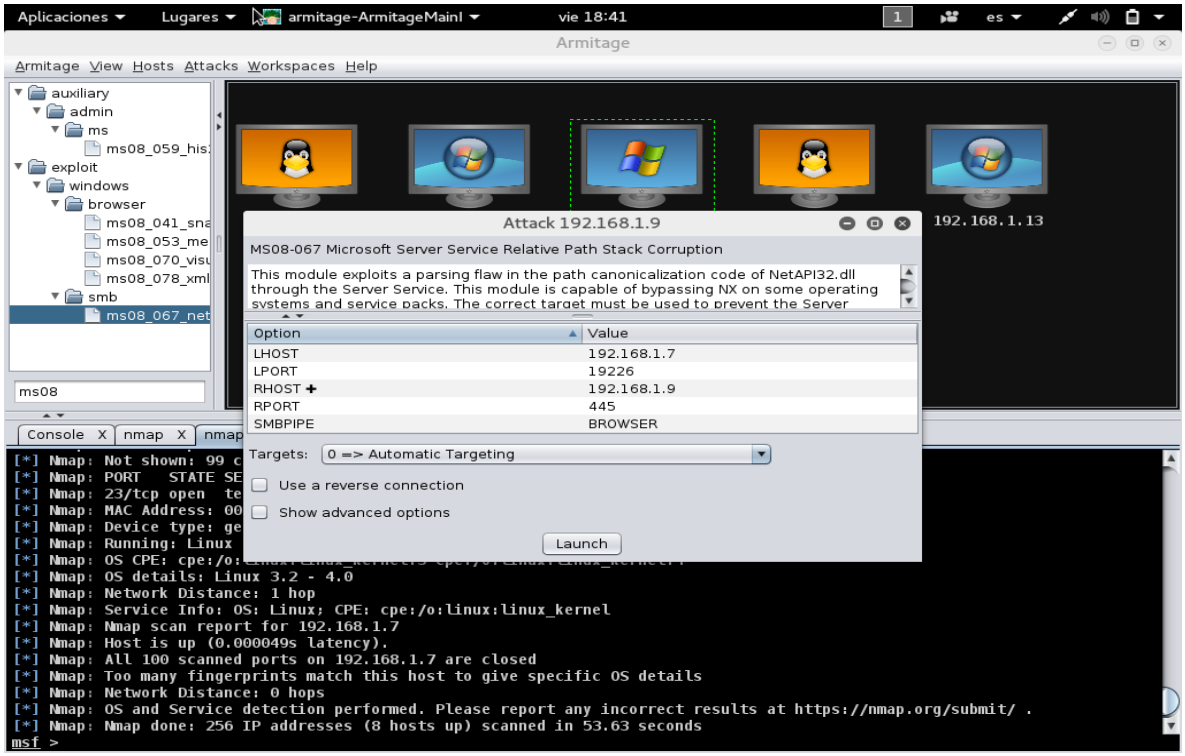
Con esto armitage selecciona el equipo y lo alista para ser explotado.

El equipo tomado tiene como sistema operativo Windows XP y este tiene una vulnerabilidad MS08-67 la cual le permite a un atacante remoto la ejecución de código maligno permitiéndole así el control de la maquina afectada poniendo en riesgo el sistema.

Para atacar la maquina realizaremos los siguientes pasos.

1. Seleccionamos la maquina Windows XP.
2. Seleccionamos el exploit correspondiente.
3. En LHOST colocaremos nuestra IP
4. En LPORT colocaremos 19229
5. En RHOST colocaremos la IP de nuestra victima
6. Seleccionamos Use a reverse connection
7. Launch

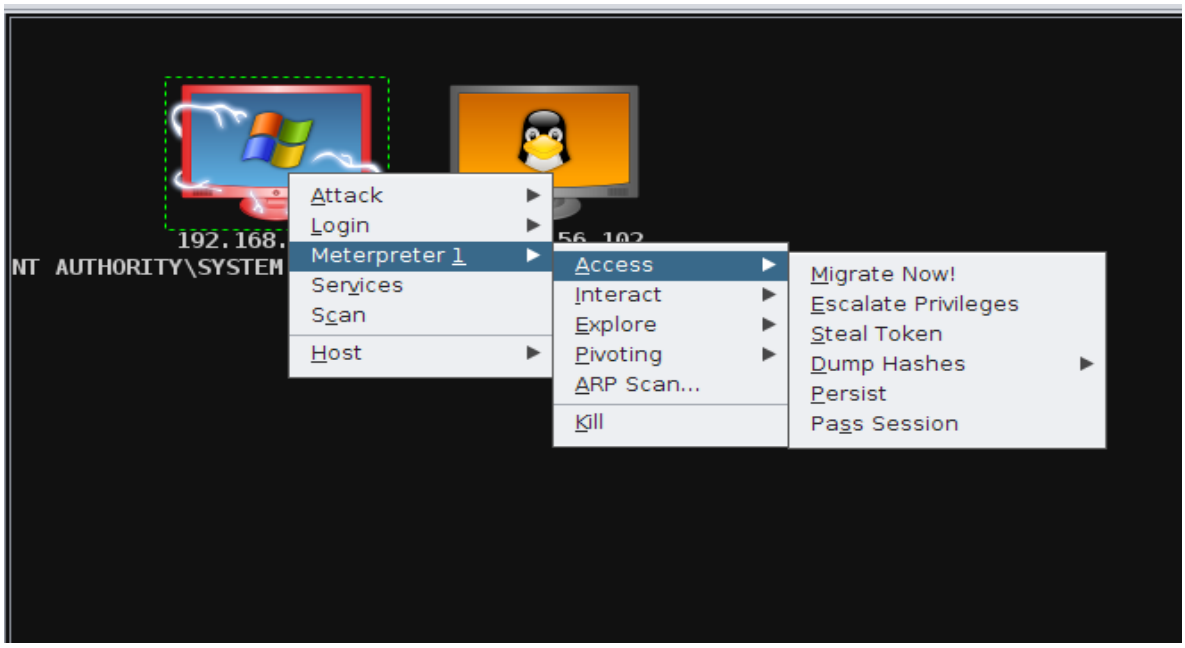
Figura 7 Explotando Vulnerabilidades



Tomada de: Autor

Una vez el equipo está comprometido se colocara en color rojo, esto significa que ahora podremos realizar distintas tareas sobre la maquina como si se tratara de un acceso remoto permitido como se muestra en la figura 8.

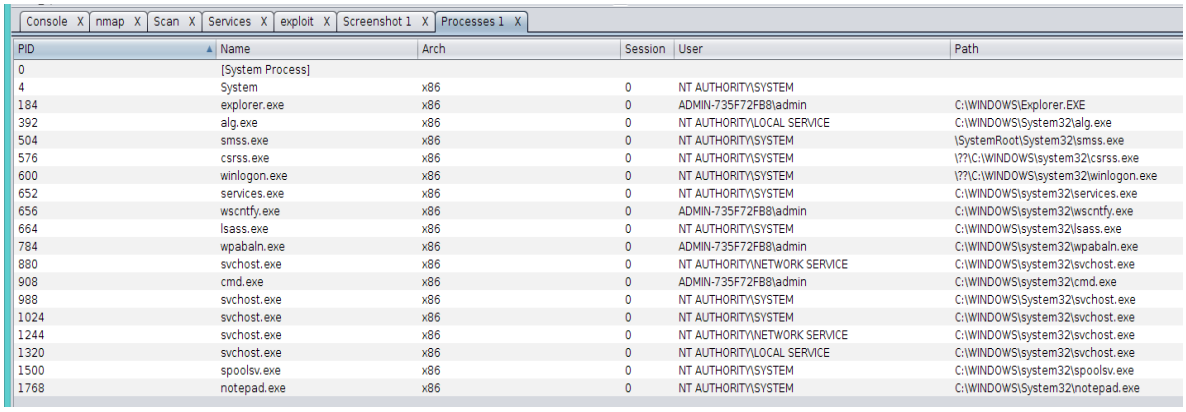
Figura 8 Iniciando Control de la Maquina



Tomada de: Autor

Podemos ver los diferentes procesos que están corriendo en la máquina podemos copiar archivos y también manipular la maquina atacada como se muestra en la figura 9.

Figura 9 Lista de Procesos en la Maquina Accedida



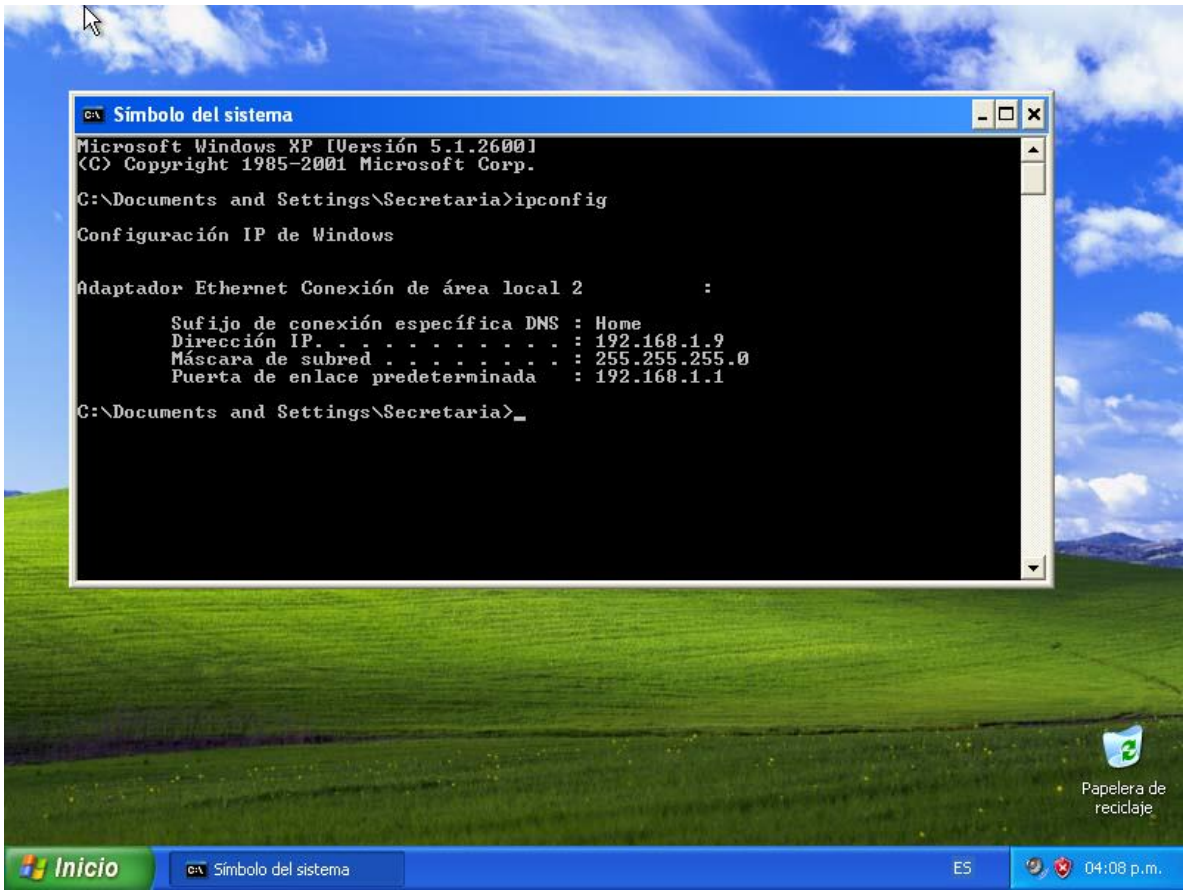
Console X | nmap X | Scan X | Services X | exploit X | Screenshot 1 X | Processes 1 X

PID	Name	Arch	Session	User	Path
0	[System Process]				
4	System	x86	0	NT AUTHORITY\SYSTEM	
184	explorer.exe	x86	0	ADMIN-735F72FB8\admin	C:\WINDOWS\Explorer.EXE
392	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
504	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
576	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
600	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
652	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
656	wscntfy.exe	x86	0	ADMIN-735F72FB8\admin	C:\WINDOWS\system32\wscntfy.exe
664	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
784	wpabaln.exe	x86	0	ADMIN-735F72FB8\admin	C:\WINDOWS\system32\wpabaln.exe
880	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
908	cmd.exe	x86	0	ADMIN-735F72FB8\admin	C:\WINDOWS\system32\cmd.exe
988	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1024	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1244	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1320	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1500	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1768	notepad.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\notepad.exe

Tomada de: Autor

Podemos copiar archivos y también manipular la maquina atacada.

Figura 10 Pantallazo de la Maquina Victima



Tomada de: Autor

5. ATAQUES A LOS QUE ESTÁ EXPUESTA LA RED

Debido al crecimiento y desarrollo tecnológico las redes de computadoras se encuentran a diario expuestas a todo tipo de ataques. Estos ataques que buscan explotar las diferentes vulnerabilidades de los sistemas a menudo son perpetrados por intrusos que quieren darle un uso diferente.

A continuación se listaran los ataques más frecuentes a los que se encuentra expuesta una red de computadoras.

5.1. ATAQUES DESTINADOS A REDES WIFI

Ningún tipo de red es 100% segura, las redes cableadas también suelen ser vulneradas. Pero las redes inalámbricas suelen ser más vulnerables debido a que su señal puede ser recibida en diferentes direcciones.

5.1.1. Access Point Spoofing

Access Point Spoofing o "Asociación Maliciosa": es un tipo de ataque en el cual la persona que está realizando el ataque se hace pasar por un Access point y la persona que está siendo atacada cree que se está conectado a una red WLAN verdadera. Este ataque en muy común en redes ad-hoc.

5.1.2. **MAC spoofing**

Este tipo de ataques suceden o se aplican cuando alguien roba una dirección MAC de una red haciéndose pasar por un cliente o usuario autorizado. En general, las placas de redes permiten el cambio de lo numero MAC por otro, lo que posibilita este tipo de ataque.

5.1.3. **ARP Poisoning**

Es una técnica utilizada para infiltrarse en una red, el objetivo del atacante es husmear paquetes de datos que pasan por la LAN, modificar el tráfico, o incluso detenerlo.

Mediante este tipo de ataques se puede obtener información valiosa sobre las posibles víctimas en la misma red en la cual se encuentra el atacante, como nombres de usuarios, contraseñas, cookies, mensajes de correo y mensajería instantánea, conversaciones, etc.

5.1.4. **WLAN escáners**

Consiste en recorrer un lugar que se desea invadir con el objetivo de descubrir redes WLAN activas en dicho lugar este tipo de ataques se conocen como ataque de vigilancia.

5.1.5. **Wardriving y warchalking**

Se le llama wardriving a la actividad de recorrer la ciudad buscando puntos de acceso a redes inalámbricas haciendo uso de una computadora portátil con una placa de red Wireless para detectar las diferentes señales.

Warchalking se le llama al hecho de marcar de alguna forma las casas que anterior mente vulneraron la red para que otros atacantes ingresen a la misma red.

5.2. **COMO REDUCIR VULNERABILIDADES EN LA RED**

Para una prevención de riesgos responsable, los administradores deben tener en cuenta las siguientes sugerencias dado que la seguridad de los sistemas a su cargo depende de su entera preocupación así como también deben capacitar a los usuarios en la navegación en la web de la siguiente manera:

No ingresar a enlaces sospechosos: es indispensable evitar ingresar a sitios web de dudosa procedencia ya que estos presentan una amenaza para los usuarios.

No ingresar a sitios WEB de los que no se tenga conocimiento: actualmente la tecnología permite que personas inescrupulosas desarrollen sitios en la web que ofrecen descuentos, promociones, beneficios que logran engañar la confianza. Se recomienda estar atento a este tipo de sitios y a los mensajes que envían los mismos y evitar ingresa a estos sitos.

Actualizar los sistemas operativos: actualizar los sistemas operativos evita que se encuentren huecos en el sistema.

Aceptar sólo contactos conocidos: es muy importante considerar los contactos de la mensajería instantánea y las redes sociales, es recomendable solo aceptar e interactuar con usuarios o contactos conocidos.

Descargar aplicaciones solo desde sitios web oficiales: Es recomendable que al momento de realizar descargas de aplicaciones, lo haga siempre desde las páginas web oficiales. Esto se debe a que muchos sitios web fingen ofrecer programas o aplicaciones populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware (software malicioso) y descargan el código malicioso al momento de instalarlo en el sistema.

Evitar la ejecución de archivos sospechosos: La proliferación de software malicioso o malware suele darse a través de archivos ejecutables (exe). Por eso es recomendable evitar la ejecución de archivos a menos que se conozca su seguridad, función y procedencia comprobando que sea confiable.

Utilizar tecnologías de seguridad: las soluciones de software o aplicaciones como antivirus, firewall y anti-spam representan las acciones más importantes para la protección del equipo ante los principales ataques o amenazas que se propagan por la red. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

Evitar el ingreso de información o datos personales en formularios dudosos: en el momento cuando el usuario afronte el diligenciamiento de un formulario web que contenga campos con información sensible (por ejemplo, usuario, contraseña, números de teléfono, números de tarjeta, etc.), es recomendable verificar la legitimidad del sitio web. Una buena estrategia es corroborar el dominio y la utilización del protocolo de seguridad HTTPS para garantizar la confidencialidad de la información.

Tener precaución con los resultados arrojados por los buscadores web: a través de técnicas como Black Hat SEO26, habitualmente los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público. Ante cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado o enrutado. Algunas características de la técnica black hat SEO son: Desafían las normas y reglas que proponen los buscadores, Interrumpen la navegación de los usuarios por las técnicas utilizadas, Páginas desordenadas, con muchas palabras visibles sin sentido para el usuario y Posibilidad de malware en el sitio web. [17]

5.3. ESTRATEGIAS DE MITIGACIÓN DE ATAQUES INFORMÁTICOS A LA RED DE COMPUTADORAS, SUS SERVICIOS Y FUNCIONARIOS.

No hay duda de que los ataques y amenazas informáticas en general, los códigos maliciosos, virus, spyware, etc. han venido evolucionando a la par de las tecnologías de información y comunicación (TIC), aumentando considerablemente el nivel de complejidad y agresión.

Es por ello necesario que todos los usuarios incorporen buenas prácticas para proteger el entorno de información, y así prevenir la posibilidad de conformar parte del conjunto que

[17] Seguridad informática (2010). Tomado de: https://www.infospyware.com/articulos/10-consejos-para-navegar-seguro-por-internet/

engrosan las potenciales y eventuales víctimas de cualquiera de las amenazas existentes, constantemente se busca sacar provecho de las debilidades humanas, por esto se deben conocer los peligros latentes, y cómo detenerlos a través de mecanismos de prevención.

Algunas medidas de seguridad que permitirán reducir ser potenciales víctimas de ataques informáticos.

5.3.1. **Mantener actualizado el sistema operativo y las aplicaciones**

El estudio del Malware41 nos brinda la respuesta del porque es importante mantener actualizados los sistemas operativos (SO) y las aplicaciones con sus respectivos parches de seguridad.

En cuanto a este aspecto de seguridad, las medidas prácticas de prevención se enfocan en:

- Nunca descargar actualizaciones desde sitios web desconocidos.
- Realice la descarga de las actualizaciones a través de los procedimientos brindados por el fabricante o programador.
- En los entornos empresariales, y sin importar la plataforma del sistema operativo, se aconseja mantener las actualizaciones activas tanto de los sistemas operativos como de las aplicaciones.

5.3.2. **Aseguramiento del sistema operativo**

Es muy importante la configuración del sistema operativo para hacerlo mucho más seguro, a continuación se relacionan las buenas prácticas que se deben tener en cuenta:

- Deshabilitar las carpetas compartidas, para evitar la propagación de gusanos o troyanos que aprovechan cualquier vulnerabilidad.
- Utilizar contraseñas fuertes para el ingreso al sistema operativo, porque el uso de contraseñas débiles permite que se penetren fácilmente.
- Crear o configurar un perfil de usuario con privilegios restringidos.
- Deshabilitar la ejecución automática de dispositivos de almacenamiento USB.
- Usar sistemas operativos modernos y de última generación, los sistemas operativos obsoletos no cuentan con soporte técnico.
- Configurar la visualización de archivos ocultos, dado que los virus se esconden en el sistema con este tipo de atributos.

5.3.3. **Protección del correo electrónico**

El uso de E-mail o correo electrónico, se convierte en uno de los medios por el cual se efectúan más ataques, por consiguiente los usuarios deben implementar buenas prácticas de uso del correo electrónico que le permitan prevenir los ataques realizados a través de códigos maliciosos.

Por consiguiente, a continuación se presenta una serie de acciones preventivas orientadas a aumentar la seguridad:

5.3.4. **Spam**

Un Spam, es un correo electrónico que promociona diferentes productos y servicios a través de publicidad no requerida o solicitada, enviada masivamente a las direcciones de correo de los usuarios.

Los Spam se han convertido en uno de los medios de propagación de virus más utilizado y por lo tanto se recomienda:

- No confiar en correos spam con archivos adjuntos y utilizar antivirus antes de ejecutarlo.
- Cuando se reciben archivos adjuntos al correo electrónico, se debe procurar y analizar las extensiones de los mismos.
- Utilizar filtros o aplicaciones anti-spam que permitan el filtrado del correo no deseado.
- Nunca responder un correo spam.
- No re-enviar mensajes en cadena, estos ser utilizados para recolectar las direcciones de correo.
- Para el envió de correos electrónicos masivos se recomienda utilizar la opción de Con Copia Oculta (CCO).
- Utilizar claves seguras y cambiar la contraseña con periodicidad si se utiliza webmail.

5.3.5. **Phishing**

Es una modalidad delictiva que se realizada a través de Internet, y consiste en robar información de incautos a través de los correos electrónicos.

Entre las acciones de seguridad que se recomiendan a los usuarios, tenemos las siguientes:

- Sospechar de los correos electrónicos enviados por entidades que brindan servicios y solicitan actualización de datos personales ya que suelen ser métodos de Ingeniería Social.
- Tener presente que las entidades bancarias y financieras nunca solicitan datos confidenciales a través de correo electrónico.
- Estar seguro de que la dirección del sitio web al cual se accede comience con el protocolo https.
- Comunicarse telefónicamente con la entidad bancaria para eliminar la posibilidad de ser víctimas de un engaño.
- Nunca se debe enviar contraseñas, números de tarjetas de débito o crédito a través del correo electrónico.

5.3.6. **Seguridad en la navegación**

Con el aumento del uso del internet, también han aumentado las acciones de ataques informáticos a través de diferentes formas y métodos, como la ingeniería social.

Es muy importante navegar en internet con mucho cuidado, por ello tenga presente las siguientes recomendaciones:

- Evitar la ejecución de archivos desde sitios web desconocidos.
- Descargar Aplicaciones o programas de seguridad solamente si es del sitio oficial del mismo.
- Configurar el navegador de internet para minimizar el riesgo de ataques a través del mismo.
- Instalar antivirus con capacidades proactivas, que permita detectar códigos maliciosos y explorar con el mismo cada archivo descargado.
- Activar el Firewall, para bloquear comunicaciones entrantes y salientes.
- Si ingresar a internet desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se haya ingresado datos.
- Bloquear sitios considerados maliciosos, ya sea porque descargan malware.

5.3.7. **Seguridad en redes sociales**

Hoy en día, las redes sociales son muy comunes y los cibernautas las utilizan masivamente; esta condición las convierte en el centro de propagación de malware.

Por tal motivo, tenga en cuenta y aplicar las siguientes acciones preventivas:

- Procurar no subir o publicar información personal o confidencial, debido a que personas extrañas pueden aprovechar esta información con fines maliciosos.
- Mantener o configurar el perfil para que no sea público.
- Nunca responder las invitaciones de desconocidos, ya que pueden contener virus.
- Ignorar los mensajes que contienen u ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de virus.
- Cambiar o modificar con frecuencia la contraseña para evitar que la misma sea descubierta fácilmente.

5.3.8. **Seguridad en mensajería instantánea**

Este medio de comunicación, se constituyen en el más utilizado para ejecutar las diferentes amenazas, dentro de las que podemos mencionar él envió de malware.

Para prevenir ser víctima de acciones maliciosas, se recomienda aplicar las siguientes medidas de seguridad:

- No aceptar como contactos a cuentas desconocidas y sin establecer a quién corresponde.
- No bajar archivos de dudosos, más aun cuando vienen acompañados de mensajes genéricos o en otro idioma.
- Configurar en el correo electrónico la exploración automática de archivos en el momento de su recepción

- No hacer clic en los enlaces dejados en el contenido del mensaje, ya que pueden direccionar a páginas con contenido malicioso o la descarga de malware.
- No digitar los datos de personales, contraseñas, claves de tarjetas, etc. en link de dudosa procedencia.
- Cambiar la contraseña de manera periódica.
- No compartir la contraseña dado que es de carácter privado e intransferible.
- No compartir información confidencial a través de este medio ya que la misma puede ser interceptada por hacker.

6. **CRONOGRAMA**

A continuación se describen las fases de desarrollo del proyecto de investigación:

Tabla 1 Cronograma

Cronograma de Actividades 2016																	
Ítem	Fases	Marzo				Abril				Mayo				Junio			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	I	X	X	X	X												
2	II			X	X	X											
3	III					X	X	X	X	X	X	X					
4	IV									X	X	X	X				
5	V											X	X	X	X		
6	VI														X	X	X

Fase I: Identificación de las diferentes fuentes de información que permitirán ampliar la perspectiva del conocimiento a aplicar.

Fase II: Análisis y clasificación de la información según su género, origen y categoría.

Fase III: Selección y aplicación de las herramientas de Pentesting “Prueba de Penetración” para determinar las vulnerabilidades de la red de computadoras y sus servicios.

Fase IV: Análisis de resultados obtenidos de la red de computadores y sus servicios e identificación de las vulnerabilidades.

Fase V: Aplicación de medidas correctivas y sugerencias para mitigar las vulnerabilidades de la red de computadora y sus servicios.

Fase VI: Conclusiones y elaboración de un Documento final.

7. RECURSOS Y PRESUPUESTO

Para el desarrollo de la investigación, se utilizaron los siguientes recursos y presupuesto:

Tabla 2 Recursos y Presupuestos

Ítem / Actividad	Cantidad	Costo Unitario	Costo Total
1. Personal			
Investigador	1	2.000.000	2.000.000
Asistentes	2	500.000	1.000.000
2. Equipos			
Computador	1	1.500.000	1.500.000
Impresora Laser	1	600.000	600.000
Internet	1xMes	50.000	200.000
3. Desplazamientos			
Transporte	1	400.000	400.000
Combustible	6	150.000	900.000
4. Materiales			
Memorias USB	1	50.000	50.000
Papelería (Lapiceros, CD, etc)	1	40.000	40.000
Fotocopias	10	30.000	300.000
Tóner de impresora	2	400.000	400.000
5. Servicios Técnicos			
Transcripción de encuestas	2	200.000	400.000

Tabla 3 (Continuación)

Ítem / Actividad	Cantidad	Costo Unitario	Costo Total
Software (Aplicaciones)	1	1.000.000	1.000.000
6. Otros			
Imprevistos	1	1.000.000	500.000
7. Total			$9.290.000

8. **CONCLUSIONES**

Con el aumento de las redes de computadoras, así mismo lo han hecho la inseguridad informática, a diario se buscan forma de estar más seguros informáticamente, pero al mismo tiempo, algunos hacker, encuentran las vulnerabilidades o debilidades.

El Pentesting “prueba de penetración” para la identificación de vulnerabilidades de la red de computadoras y sus servicios en la alcaldía del municipio de Cantón de san pablo, departamento del Chocó, permitió llegar a las siguientes conclusiones:

- Los sistemas operativos de los equipos de cómputo de los usuarios no se encuentran actualizados para mitigar las vulnerabilidades y los riegos de ataques.
- Las contraseñas utilizadas por los funcionarios para el acceso a los sistemas de información no cuentan con estructuras seguras, difíciles de romper o descifrar.
- El Sistema operativo Linux BackTrack contiene muchas herramientas que permiten monitorear y ayudar a proteger la red de computadoras.
- La estructura física de la red requiere mejorar las condiciones del cableado y del centro de comunicaciones.
- No se cuenta con medidas de seguridad guiados y documentados, por lo cual este estudio será de gran ayuda para minimizar los impactos generados por los códigos maliciosos o malware.

A su vez, es importante reconocer que la mayoría de los ataques son suscitados por amenazas internas, específicamente de los funcionarios, reduciendo la hipótesis que da como origen que las amenazas son externas, Es evidente que no se puede llegar a tener un 100% de seguridad informática, pero aplicando algunas de las estrategias de protección se obtendrá una seguridad aceptable de acuerdo a las necesidades que surgen dentro de la entidad.

9. **RECOMENDACIONES**

- Se debe informar a los funcionarios de la Alcaldía de Cantón de san pablo los nombres de las redes inalámbricas generadas por los Access Point (AP), de esa forma se evita que se conecten a redes diferentes a las autorizadas y pueden ser víctimas de robos sus contraseñas.
- Implementar políticas de seguridad acorde a las necesidades y exigencias de los administradores de sistemas.
- Se deben brindar capacitaciones en seguridad de la información a los funcionarios.
- Restringir el uso de dispositivos de almacenamiento extraíbles que se conectan a través del puerto USB, para evitar la propagación de virus o códigos maliciosos.
- Implementar el uso de Antivirus licenciado para contrarrestar la propagación de códigos maliciosos o malware.

10. **REFERENCIAS BIBLIOGRÁFICAS**

ARRIETA, G. J. (1998) *Medidas para aumentar la seguridad informática en el centro de trabajo*. Obtenido de Slideshare: http://es.slideshare.net/mariorafaelquirozmartinez/medidas-para-aumentar-la-seguridad-informatica-en-su-centro-de-trabajo

ALFONSO E. OTEO (2014). *Tipos de Ataques Informáticos.* Obtenido de: http://www.coreoneit.com/tipos-de-ataques-informaticos/

CARRASCO, F. (2011) *90 % de las empresas han sido víctimas de vulnerabilidades de Seguridad*. Obtenido de CIO América Latina: http://www.cioal.com/2011/06/30/90-de-las-empresas-han-sido-victimas-de-vulnerabilidades-de-seguridad/

CRIATIAN BORGHELLO (2009). *Amenazas Lógicas – Tipos de ataques*. Obtenido de: http://www.segu-info.com.ar/ataques/ataques.htm

DAVID A. FRANCO, JORGE L. PEREA & LUIS C. TOVAR. (2013). *Herramientas para la Detección de Vulnerabilidades basada en la identificación de servicios*. Obtenido de: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext

DAZA TRIANA, S. M., & GIRALDO MURILLO, M. A. (2012) *Aplicación de un sistema de gestión de vulnerabilidades para la infraestructura informática de ABC Ltda*. Obtenido de Escuela de Administración de negocios: http://repository.ean.edu.co/bitstream/10882/2590/1/DazaSandra2012.pdf

FRANCO, D. A., PEREA, J.L., & TOVAR, L. C. (2013) *Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios*. Obtenido de Scielo: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext

FERNANDO CATORIRA (24 de Julio de 2012). *Penetration Test, ¿En qué consiste?* Obtenido de: http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

GONZALES, J. C. (2013) *Vulnerabilidades de seguridad en las empresas*. Obtenido de Universidad autónoma de Nuevo León: http://eprints.uanl.mx/3567/1/VULNERABILIDADES_DE_SEGURIDAD_EN_LAS_EMPRESAS.pdf

HERRERA STEFANI D. (11 de Abril de 2013). *Vulnerabilidad de los Sistemas Informáticos*. Tomado de: http://vulnerabilidadtisg.blogspot.com/

MAURO MAULINI, (04 de Diciembre de 2010). *Desarrollo y Seguridad de Aplicaciones web y Móviles*. Obtenido de: http://tecnologiasweb.blogspot.com/2010/12/que-es-pen-test-herramientas-de-pen.html

MIFSUD, E. (2012) MONOGRÁFICO: *Introducción a la seguridad informática - Vulnerabilidades de un sistema informática*. Obtenido de Recursostic: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

MYERSON, J. (2012) Servicios en la nube: *mitigar riesgos, mantener la disponibilidad*. Obtenido de IBM: http://www.ibm.com/developerworks/ssa/cloud/library/cl-cloudservicerisks/

ROMERO, A. (2011) *Aspectos Básicos de la Seguridad en Aplicaciones Web*. Obtenido de Coordinación de Seguridad de la Información: http://www.seguridad.unam.mx/documento/?id=17

SEGURIDAD INFORMÁTICA. (19 de Abril de 2014). *Seguridad Informatica* (Ethical Hacksing, Pen-test, Anti Script-Kiddies). Tomado de: http://antisec-security.blogspot.mx/2014/04/webpwn3r-webapps-security-scanner.html

SEGURIDAD INFORMÁTICA. (2014). *Vulnerabilidades de un sistema Informático*. Tomado de: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/ud1_introduccin_a_la_seguridad_informtica.html

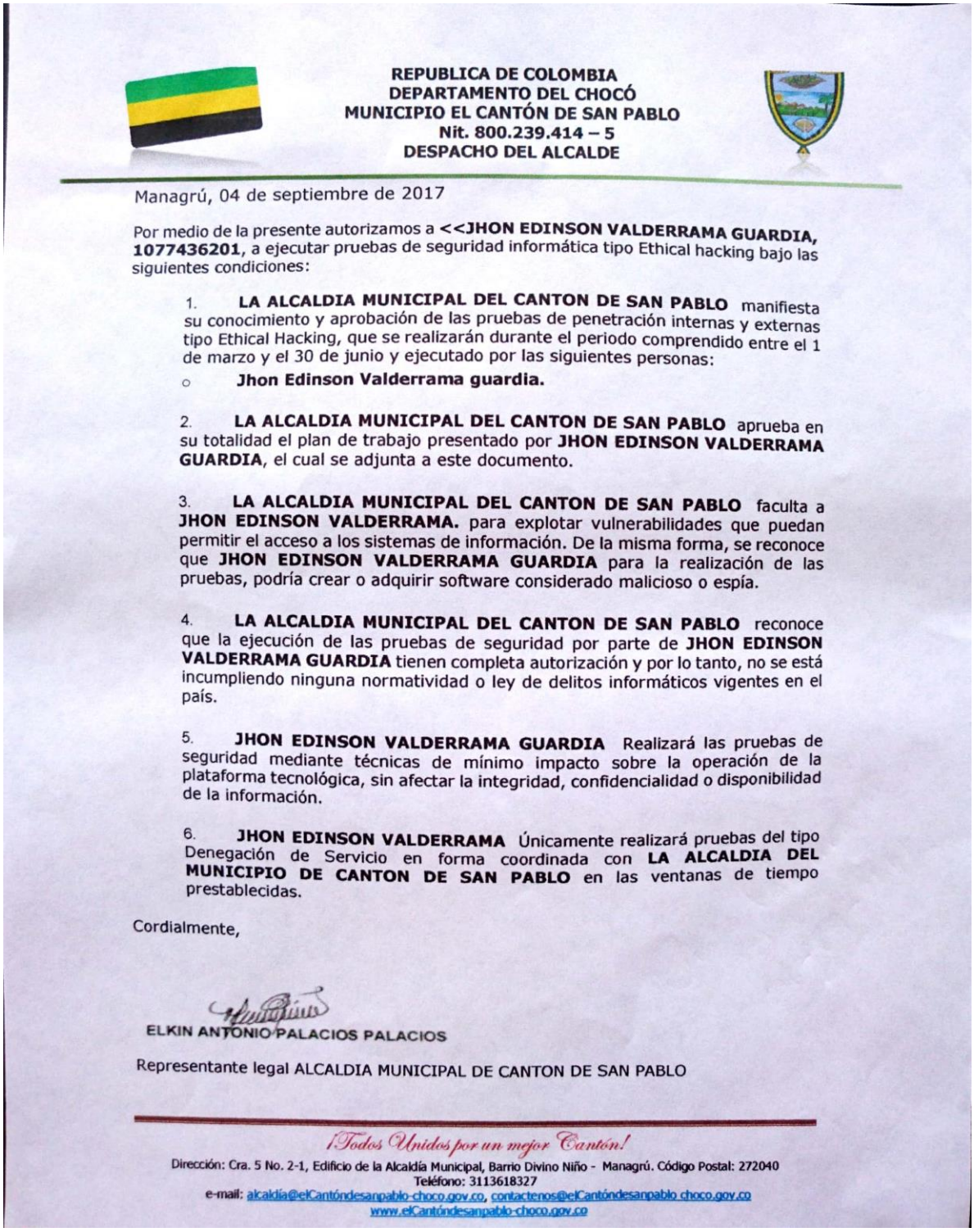
SERRANO, M. (2011) *Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala*. Obtenido de Universidad Javeriana: http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf

Toni Puig. (20 de Mayo de 2008). *Gestión de Riesgos de los Sistemas de Información.* Obtenido de: http://www.mailxmail.com/curso-gestion-riesgos-sistemas-informacion/identificacion-vulnerabilidades-impactos

UTRERAS, JAVIER. (09 de 04 de 2012). *Seguridad de la Información*. Obtenido de YouTube: http://www.youtube.com/watch?v=_nKXEWIfHDo

11. **ANEXOS**

Anexo A. Permiso de la Alcaldía El cantón de San Pablo, Chocó



REPUBLICA DE COLOMBIA
DEPARTAMENTO DEL CHOCÓ
MUNICIPIO EL CANTÓN DE SAN PABLO
Nit. 800.239.414 – 5
DESPACHO DEL ALCALDE

Managrú, 04 de septiembre de 2017

Por medio de la presente autorizamos a **<<JHON EDINSON VALDERRAMA GUARDIA, 1077436201**, a ejecutar pruebas de seguridad informática tipo Ethical hacking bajo las siguientes condiciones:

1. **LA ALCALDIA MUNICIPAL DEL CANTON DE SAN PABLO** manifiesta su conocimiento y aprobación de las pruebas de penetración internas y externas tipo Ethical Hacking, que se realizarán durante el periodo comprendido entre el 1 de marzo y el 30 de junio y ejecutado por las siguientes personas:
   - **Jhon Edinson Valderrama guardia.**

2. **LA ALCALDIA MUNICIPAL DEL CANTON DE SAN PABLO** aprueba en su totalidad el plan de trabajo presentado por **JHON EDINSON VALDERRAMA GUARDIA**, el cual se adjunta a este documento.

3. **LA ALCALDIA MUNICIPAL DEL CANTON DE SAN PABLO** faculta a **JHON EDINSON VALDERRAMA.** para explotar vulnerabilidades que puedan permitir el acceso a los sistemas de información. De la misma forma, se reconoce que **JHON EDINSON VALDERRAMA GUARDIA** para la realización de las pruebas, podría crear o adquirir software considerado malicioso o espía.

4. **LA ALCALDIA MUNICIPAL DEL CANTON DE SAN PABLO** reconoce que la ejecución de las pruebas de seguridad por parte de **JHON EDINSON VALDERRAMA GUARDIA** tienen completa autorización y por lo tanto, no se está incumpliendo ninguna normatividad o ley de delitos informáticos vigentes en el país.

5. **JHON EDINSON VALDERRAMA GUARDIA** Realizará las pruebas de seguridad mediante técnicas de mínimo impacto sobre la operación de la plataforma tecnológica, sin afectar la integridad, confidencialidad o disponibilidad de la información.

6. **JHON EDINSON VALDERRAMA** Únicamente realizará pruebas del tipo Denegación de Servicio en forma coordinada con **LA ALCALDIA DEL MUNICIPIO DE CANTON DE SAN PABLO** en las ventanas de tiempo prestablecidas.

Cordialmente,

ELKIN ANTONIO PALACIOS PALACIOS

Representante legal ALCALDIA MUNICIPAL DE CANTON DE SAN PABLO

¡Todos Unidos por un mejor Cantón!

Dirección: Cra. 5 No. 2-1, Edificio de la Alcaldía Municipal, Barrio Divino Niño - Managrú. Código Postal: 272040
Teléfono: 3113618327
e-mail: alcaldía@elCantóndesanpablo-choco.gov.co, contactenos@elCantóndesanpablo.choco.gov.co
www.elCantóndesanpablo-choco.gov.co

RESUMEN ANÁLITICO RAE.

Tema	Investigación, con el objetivo de conocer las diferente vulnerabilidades de la alcaldía de canton de san pablo.
Título de Documento.	Pentesting “prueba de penetración” para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de cantón del san pablo, departamento del chocó
Año	
Autor	Valderrama Guardia Jhon Edinson
Palabras Claves	Backtrack, Cracker, Criptografía Denegación de Servicio, Exploits, Firewall, Hacker, Ingeniería Social, Nessus, Netbios, Nmap, TCP, TCP/IP, Test de Penetración, Xploit
Fuentes Bibliográficas	DAVID A. FRANCO, JORGE L. PEREA & LUIS C. TOVAR. (2013). *Herramientas para la Detección de Vulnerabilidades basada en la identificación de servicios*. Obtenido de: http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext FERNANDO CATORIRA (24 de Julio de 2012). *Penetration Test, ¿En qué consiste?* Obtenido de: http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/ GONZALES, J. C. (2013) *Vulnerabilidades de seguridad en las empresas*. Obtenido de Universidad autónoma de Nuevo León: http://eprints.uanl.mx/3567/1/VULNERABILIDADES_DE_SEGURID

	AD_EN_LAS_EMPRESAS.pdf HERRERA STEFANI D. (11 de Abril de 2013). *Vulnerabilidad de los Sistemas Informáticos*. Tomado de: http://vulnerabilidadtisg.blogspot.com/ MIFSUD, E. (2012) MONOGRÁFICO: *Introducción a la seguridad informática - Vulnerabilidades de un sistema informática*. Obtenido de Recursostic: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3 SEGURIDAD INFORMÁTICA. (19 de Abril de 2014). *Seguridad Informatica* (Ethical Hacksing, Pen-test, Anti Script-Kiddies). Tomado de: http://antisec-security.blogspot.mx/2014/04/webpwn3r-webapps-security-scanner.html
Objetivos del proyecto	

Contenido:

a) Descripción del problema: realizar diferentes pruebas de penetración para conocer las diferente vulnerabilidades que tiene la red local en la alcaldía de canton del san pablo.
b) Objetivo General. Describir los problemas de seguridad de la red de computadoras en la alcaldía del municipio de Cantón de san Pablo, a través de pruebas de penetración que permitan el mejoramiento continuo de la entidad.
c) Objetivos Específicos.

- Realizar un pentesting "prueba de penetración" para la determinar qué tipo de vulnerabilidades presenta la red de computadoras en la alcaldía del municipio de Cantón de san Pablo, departamento del Chocó.
- Identificar los diferentes ataques a los que está expuesta la red de computadoras y sus servicios.
- Generar recomendaciones que reduzcan la vulnerabilidad de la red de computadoras.

d) Resumen de lo desarrollado en el proyecto.

Metodología

Descripción de la metodología que usaron para el desarrollo del proyecto.

Resultados

Conclusiones

- Los sistemas operativos de los equipos de cómputo de los usuarios no se encuentran actualizados para mitigar las vulnerabilidades y los riegos de ataques.
- Las contraseñas utilizadas por los funcionarios para el acceso a los sistemas de información no cuentan con estructuras seguras, difíciles de romper o descifrar.
- El Sistema operativo Linux BackTrack contiene muchas herramientas que permiten monitorear y ayudar a proteger la red de computadoras.
- La estructura física de la red requiere mejorar las condiciones del cableado y del centro de comunicaciones.
- No se cuenta con medidas de seguridad guiados y documentados, por lo cual este estudio será de gran ayuda para minimizar los impactos generados por los códigos maliciosos o malware.

Recomendaciones.

- Se debe informar a los funcionarios de la Alcaldía de Cantón de san pablo los nombres de las redes inalámbricas generadas por los Access Point (AP), de esa forma se evita que se conecten a redes diferentes a las autorizadas y pueden ser víctimas de robos sus contraseñas.
- Implementar políticas de seguridad acorde a las necesidades y exigencias de los administradores de sistemas.
- Se deben brindar capacitaciones en seguridad de la información a los funcionarios.
- Restringir el uso de dispositivos de almacenamiento extraíbles que se conectan a través del puerto USB, para evitar la propagación de virus o códigos maliciosos.
- Implementar el uso de Antivirus licenciado para contrarrestar la propagación de códigos maliciosos o malware.